**Yee &
Associates, P.C.**

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Philip C. Lee Group Art Unit 2154**	Facsimile No.: **703/872-9306**
From: Monica Gamez Legal Assistant to Ted Fay	No. of Pages Including Cover Sheet: **40**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. 09/726,266

Attorney Docket No: AUS9-2000-0486-US1

Date: Wednesday, February 16, 2005

| **Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.** | *This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.* |

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Pratt et al.**

Serial No.: **09/726,266**

Filed: **November 30, 2000**

For: **Method for Managing Resources on a Per User Basis for UNIX Based Systems**

§
§
§
§
§
§

Group Art Unit: **2154**
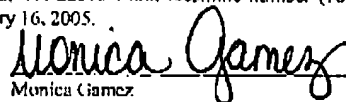
Examiner: **Lee, Philip C.**

Attorney Docket No.: **AUS9-2000-0486-US1**

```
┌─────────────────────────────────────────────────────────┐
│    Certificate of Transmission Under 37 C.F.R. § 1.8(a)  │
│ I hereby certify this correspondence is being transmitted via facsimile to │
│ the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313- │
│ 1450, facsimile number (703) 872-9306 on February 16, 2005. │
│                                                           │
│ By:    Monica Gamez                                       │
│            Monica Gamez                                    │
│                                                           │
└─────────────────────────────────────────────────────────┘
```

35525

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL DOCUMENT

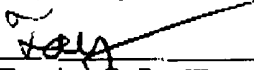Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

• Appeal Brief (37 C.F.R. 41.37).

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Theodore D. Fay III
Registration No. 48,504
Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

Docket No. AUS9-2000-0486-US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Pratt et al.**	§	
	§	Group Art Unit: **2154**
Serial No. **09/726,266**	§	
	§	Examiner: **Lee, Philip C.**
Filed: **November 30, 2000**	§	
	§	Attorney Docket No.: **AUS9-2000-0486-US1**
For: **Method for Managing Resources**	§	
on a Per User Basis for UNIX Based	§	
Systems		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on December 16, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

Appeal Brief Page 1 of 38
Pratt et al. – 09/726,266

PAGE 3/21 * RCVD AT 2/16/2005 4:47:17 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):05-30

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines

Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by,

or have a bearing on the Board's decision in the pending appeal, there are no such appeals or

interferences.

Appeal Brief Page 3 of 38
Pratt et al. - 09/726,266

PAGE 5/21 * RCVD AT 2/16/2005 4:47:17 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):05-30

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

The claims in the application are: 1-28

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 4, 13, 14, 16, and 17

2. Claims withdrawn from consideration but not canceled: None

3. Claims pending: 1-3, 5-12, 15, and 18-28

4. Claims allowed: None

5. Claims rejected: 1-3, 5-12, 15, and 18-28

C. CLAIMS ON APPEAL

The claims on appeal are: 1-3, 5-12, 15, and 18-28

STATUS OF AMENDMENTS

No Amendments have been filed subsequent to the rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

A.   CLAIM 1 - INDEPENDENT

The subject matter of claim 1 is directed to a method for managing resources on a computer network. A configuration file is created for each user on the network. When a user logs onto a local client computer, the user identity is matched to the configuration file. Based on the configuration file, the user is allowed access to particular resources on the local client computer. In the UNIX Operating System, all resources must be attached at the local computer. What the method of claimed invention does is set up a configuration file for each user. The configuration file allows a user to attach quickly resources to which he is supposed to have access. Thus, the method of claim 1 allows users to access an individualized configuration of network resources from any client within the network, rather than limiting the configuration to one particular client. Support for claim 1 may be found on page 9, line 22 through page 10, line 30 and in Figure 4.

B.   CLAIM 18 – INDEPENDENT

Claim 18 is directed to a computer program product in a computer readable medium for carrying out the method claimed in claim 1. Support for claim 18 may be found in page 9, line 22 through page 10, line 30 and in Figure 4.

C.   CLAIM 27 - INDEPENDENT

Claim 27 is directed to a system for managing resources on a computer network where the system is designed to carry out the method of claim 1. Support for claim 27 may be found on page 9, line 22 through page 10, line 30 and in Figure 4.

The means for defining the contents for a configuration file may be found on page 10, lines 9 through 12. The support for a means for receiving a login identification for user may be found in network 102 shown in Figure 1 and described on page 5, line 4 through page 6, line 21. The means for matching the user identity with the user configuration file may be found in Figure 2 and specifically processors 202 and 204 in Figure 2, which are described on page 6, line 25 through page 7, line 5. The means for attaching network resources to a client computer based on the user identity and contents of the user configuration file may be found in Figure 1, specifically network 102, which is described on page 5, line 5 through page 6, line 21. Support for the term "wherein said computer network is configured to run on an operating system that includes an attachment of resources to a given computer to be formed on said given computer" may be found on page 1, lines 24 through 30.

C. CLAIM 28 – DEPENDENT

Support for "means for receiving a log out command from the user" may be found in network 102 shown in Figure 1 and described on page 5, line 4 through page 6, line 21. The means for matching the user identity with the user configuration file may be found in Figure 2 and specifically processors 202 and 204 in Figure 2, which are described on page 6, line 25 through page 7, line 5.

Support for "means for unattaching the attached resources to a client computer based on the user identity and contents of the user configuration file" may be found in Figure 1, specifically network 102, which is described on page 5, line 5 through page 6, line 21. Support for the term "wherein said computer network is configured to run on an operating system that includes an attachment of resources to a given computer to be formed on said given computer" may be found on page 1, lines 24 through 30.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.   GROUND OF REJECTION 1 (Claims 1-3, 5-9, 15, 18-23 and 27)

Claims 1-3, 5-9, 15, 18-23, and 27 are rejected under 35 U.S.C. § 103(a) as being obvious over

Pereira, <u>System and Method for Controlling Access to Personal Computer System Resources</u>, U.S.

Patent 5,809,230 (Sep. 15, 1998) in view of Win et al, <u>Administrative Roles That Govern Access to</u>

<u>Administrative Functions</u>, U.S. Patent 6,161,139 (Dec. 12, 2000).

B.   GROUND OF REJECTION 2 (Claims 10-11, 24-25 and 28)

Claims 10-11, 24-25 and 28 are rejected under 35 U.S.C. § 103(a) as being obvious over Pereira

and Winn in view of Hudson et al, <u>System and Method for Accessing Enterprise Wide Resources</u>

<u>by Presenting to the Resource a Temporary Credential</u>, U.S. Patent 6,055,637 (Apr. 25, 2000).

C.   GROUND OF REJECTION 3 (Claims 12 and 26)

Claims 12 and 26 are rejected under 35 U.S.C. § 103(a) as being obvious over Pereira and Win

in view of Bauer et al, <u>Method for Controlling Resource Usage by Network Identities</u>, U.S. Patent

5,819,047 (Oct. 6, 1998).

ARGUMENT

A.   GROUND OF REJECTION 1 (Claims 1-3, 5-9, 15, 18-23 and 27)

A.1.   Claims 1, 18 and 27

A.1.1. THE PROPOSED COMBINATION DOES NOT RESULT IN THE CLAIMED

INVENTIONS.

The examiner rejects claims 1, 18 and 27 under the assertion that:

> 7.   As per claims 1, 18 and 27, Pereira taught the invention
> substantially as claimed for managing resources in a computer network;
> comprising:
>> receiving a login identification from a user on a given
>> computer that uses a given operating system, wherein said given
>> operating system requires that attachment of resources to said
>> given computer be performed on said given computer (col. 1, lines
>> 47-54; col. 7, lines 10-37; col. 9, lines 34-col. 10, line 33);
>> matching the user identity with said user configuration file
>> (col. 1, lines 47-54; col. 7, lines 10-37; col. 9, line 34-col.10, line
>> 33); and
>> in response to said matching step, executing a resource
>> attachment program on said given computer to attach network
>> resources to said given computer based on the user identity and the
>> contents of said user configuration (col. 1, lines 47-54; col. 7, lines
>> 10-37; col. 9, line 34-col.10, line 33).

> 8.   Pereira did not teach defining configuration file for each network
> user. Win taught a similar system comprising:
>> defining the contents of a configuration file for each
>> network user (col. 12, lines 45-50; col. 15, lines 30-37).

> 9.   It would have been obvious to one having ordinary skill in the art
> at the time of the invention was made to combine the teachings of Pereira
> and Win because Win's system of defining configuration file for each
> network user would increase the functionality of Pereira's system by
> providing resource access control for user accessing a computer over the
> network (col. 2, lines 35-49).

Office Action of October 22, 2004, pages 3-4, paragraphs 7, 8, and 9.

The examiner has failed to state prima facie obviousness rejections because the proposed

combination does not result in the claimed inventions. Neither Pereira nor Win show defining the

contents of a configuration file for each network user. In addition, the examiner has failed to state

how either reference shows defining the contents of a configuration file for each network user. The

examiner asserts that Win does teach defining the contents of a configuration file for each network

user, citing Win as follows:

> Administration Application 114 is used by administrators to configure
> server components of the system, to set up user and resource records,
> assign roles to users and resources and manage changes to the system. The
> Administration Application provides these services by reading and writing
> information in Registry Server 108.

Win, col. 12, lines 45-50.

> Preferably, the Administration Application 114 can display a User
> Information data entry form that accepts information defining a user. An
> administrator may complete and submit the data entry form for each
> individual user to be defined. In response, Registry Server 108 stores
> information defining the user in the Registry Repository 110. Each user is
> defined by personal information, login and password information, and
> account information."

Win, col. 15, lines 30-37.

For the reference to column 12, the cited text does not show creating a configuration file for

each network user. Instead, the cited text merely shows that data on users, resources and roles in

configuration information may be stored in a registry repository. Storing configuration information

in a registry repository does not create a configuration file for each user. Win shows a centralized

database stored on a single server and not a configuration file for each user. Similarly, the text cited

from column 15 states registry server 108 stores information defining a user in the registry

repository. Each user is defined by personal information, but the information is contained in a

single database. A configuration file is not created for each user. This fact is shown in column 12,

lines 20-29, which provides as follows:

> Registry Repository 110 is the primary data store for the system 2. It
> contains data on Users, Resources and Roles and configuration
> information required for the system 2 to function. Selected data, for
> example, passwords, are stored in Registry Repository 110 in encrypted
> form. The data about Users, Resources and Roles stored in Registry
> Repository 110 represents the structure of an enterprise or organization
> that has protected resources. Data in Registry Repository 110 is managed
> using Administration Application 114.

Win, col. 12, lines 20-29

Because neither reference shows defining the contents of a configuration file for each network

user, and because the examiner has failed to provide any reason why defining the contents of a

configuration file for each network user would be obvious or even desirable, the proposed

combination does not result in the claimed inventions. Accordingly, the examiner has failed to state

prima facie obviousness rejections.

In addition, neither reference shows where the operating system described in either Pereira or

Win requires attachment of resources on a computer network to the given computer to be

performed on the given computer as claimed in claim 1. The examiner asserts that Pereira does

show these claimed steps citing the following text:

> Thus, there is a need to segregate files for one user on a PC from the other
> users. One way to keep a user from accessing certain files is to keep the
> user from gaining access to the application program that modifies the
> content of the file. Programs which control access to application programs
> are known which require a user to enter a password before the operating
> system activates the program for the user.

Pereira, col. 1, lines 47-54.

> The system initialization file probably continues by verifying that the user
> bringing up the system is authorized for use of the system. If the user is
> authorized, installation of the programs necessary for the operating system
> and the user interface continues. Control is then transferred to the user
> interface so the user may begin to select programs for execution and use. If
> the user is not authorized for system use, the system initialization program
> denies the user access. After a predetermined number of attempts to gain
> access have failed, the program aborts system initialization.

> Preferably, the resource control system and method of the present

Appeal Brief Page 11 of 38
Pratt et al. – 09/726,266

PAGE 13/21 * RCVD AT 2/16/2005 4:47:17 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):05-30

invention are implemented by an access control program which is installed
on the PC once a user is given access to the system. The program is
typically provided on a diskette which is placed in the disk drive of a PC
system. The diskette is provided with an installation program which
creates a directory for the access control program on the user's hard disk
drive. The files containing the program components are then copied into
this directory. Part of the installation procedure is to insert commands into
a system initialization file, such as the AUTOEXEC.BAT file, before the
command which activates an operating system or Windows interface
program. These commands activate the program components of the access
control program before the operating system or Windows interface
program is activated at system initialization. After the access control
program is installed, the program requests the user to register as the
Primary User and to identify a password. This password is used to identify
the Primary User at subsequent logins.

Pereira, col. 7, lines 10-37.

By activating the ports tab 82, the ports program component generates a
list of the communication and printer ports available on the system. An
exemplary display is shown in FIG. 7. Those communication and printer
ports which have an "X" in the window next to a port identifier, such as
COM1, indicate that those communication and printer ports have been
restricted from use for that user. In response to the definition of these ports
as being restricted or not, the access control program generates a file
identified by the user's identifier of ports to which the user is denied
access.

The restricted lists for the groups, programs, directories, and ports are
placed in files which are associated with a user's identifier. These files are
then used by the access control program to modify system files when a
user signs on the system. Specifically, after system initialization has been
performed by the BIOS, control is transferred to the access control
program. This program prompts the user for a user name and
corresponding password. If the password and user name are verified, the
files containing the lists of restricted groups, programs, directories, and
ports are read by the access control program. The access control program
uses the group and program lists to delete references to those files from the
system files. In the Windows 3.x environment this is done by passing the
lists to the dynamic data exchange (DDE) which causes the program
manager to delete the specified resources from the Group and INI files.
Thereafter, the only group folders and program icons which are displayed
are those which were not deleted at user sign on. The access control
program also monitors calls to the DDE and program manager to prevent
the restoration of deleted resources to the system files by a user. The
directory and port lists are used to generate tables for the program
components of the access control program which control the I/O routines

Appeal Brief Page 12 of 38
Pratt et al. – 09/726,266

PAGE 14/21 * RCVD AT 2/16/2005 4:47:17 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):05-30

that interface with the drives and ports of the PC system. These tables are maintained in memory with the program components and remain active regardless of whether the operating system or Windows interface program is executing since the DPMI is used to make the memory in which the program components are located accessible. When the program components trap a request for a directory or port, the I/O routine of the program component verifies that the requested directory or port is authorized for the user currently on the system.

In the Windows 95 environment, the access control program modifies the registry file since this file is used to define the computer resources which a user can access and which the Windows 95 program accesses to generate displays of program icons and program groups. Because Windows 95 performs its own user login procedure, the transfer from the login procedure to the access program is done differently. The login procedure in Windows 95 assigns the user a default user registry file if the user cannot enter a password that corresponds with a user's identifier or if the user aborts the login procedure. To prevent this default user from gaining control of the system, the access control program modifies the default user profile in the registry file so the default user is not authorized to use any system resources. If the user enters a corresponding password, however, the files identified by the user's identifier are used to define the resources in the registry file. Since Windows 95 uses this file to display program icons and program groups, the system only displays the ones which the Primary User identified for the user through the access control program. The access control program may use an application program interface (API) to modify the registry system file in accordance with the restricted list files generated by the access control program.

Pereira, col. 9, line 34 through col. 10, line 33.

The examiner misapprehends Pereira. Pereira does not show that the given operating system requires that attachment of network resources to a given computer be performed on said given computer, as claimed. Pereira only discusses a method for controlling access to a personal computer by adjusting the boot record in the computer. Pereira does not discuss networks at all. Thus, the cited text provides absolutely no indication that the operating system requires attachment of network resources in a computer network to be performed on that computer. Win fails to cure the lack of disclosure in Pereira. Therefore, the examiner has failed to state a prima facie obviousness rejection of claims 1, 18, and 27, which all contain similar limitations.

Appeal Brief Page 13 of 38
Pratt et al. – 09/726,266

PAGE 15/21 * RCVD AT 2/16/2005 4:47:17 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):05-30

In addition, the examiner has failed to state prima facie obviousness rejections because the examiner has failed to state a proper motivation to combine the references. A proper *prima facie* case of obviousness cannot be established by combining the teachings of the prior art absent some teaching, incentive, or suggestion supporting the combination. *In re Napier*, 55 F.3d 610, 613, 34 U.S.P.Q.2d 1782, 1784 (Fed. Cir. 1995); *In re Bond*, 910 F.2d 831, 834, 15 U.S.P.Q.2d 1566, 1568 (Fed. Cir. 1990). Regarding claims 1, 18 and 27, the examiner states that:

> 9. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Pereira and Win because Win's system of defining configuration file for each network user would increase the functionality of Pereira's system by providing resource access control for user accessing a computer over the network (col. 2, lines 35-49).

Office Action of October 22, 2004, pages 3-4, paragraph 9.

The examiner's logic depends on an incorrect evaluation of both Pereira and Win. Therefore, the statement cannot serve as a motivation to combine the references. Because the examiner has not stated a proper motivation to combine the references, the examiner has failed to state prima facie obviousness rejections.

Furthermore, one of ordinary skill in the art would recognize that the combination of Pereira and Win would be impracticable. Pereira is directed to a method of controlling access to a single computer's resources by controlling the computer's boot record. Win is directed to storing information that defines administration roles over a network. For Win and Pereira to be combined, each local computer would have to be re-booted every time a new user attempted to access the computer over a network. No one would be motivated to waste time, effort, and money by rebooting every local computer each time a new user logs in. Thus, one of ordinary skill would recognize that the examiner's statement makes no sense. Accordingly, the examiner has failed to

state prima facie obviousness rejections. For this reason, the examiner has again failed to state prima facie obviousness rejections.

In addition, the examiner's statement only provides a purported advantage to combine the references but does not state why one of ordinary skill in the art would be motivated to either recognize or implement the advantage. Furthermore, the statement misses the point of the invention and therefore does not serve as a motivation at all. Because the examiner has failed to state a proper motivation to combine the references, the examiner has failed to state prima facie obviousness rejections of claims 1, 18, and 27.

Moreover, because one of ordinary skill would recognize that the examiner's proposed combination is impracticable and because the examiner's statement does not serve as a motivation, the examiner must have used Applicants' own disclosure when fashioning the rejections. Thus, the examiner has used impermissible hindsight to fashion the rejections. In determining obviousness, an applicant's teachings may not be read into the prior art. *Panduit Corp. v. Denison Mfg. Co.*, 810 F.2d 1561, 1575 n. 29, 1 U.S.P.Q. 1593, 1602 n. 29 (Fed. Cir. 1987) (citing need to "guard against hindsight and the temptation to read the inventor's teachings into the prior art"). A determination of the desirability of combining prior art references must be made without the benefit of hindsight afforded by an applicant's disclosure. *In re Paulsen*, 30 F.3d 1475, 1482, 31 U.S.P.Q. 1671, 1676 (Fed. Cir. 1994). Accordingly, the examiner has again failed to state prima facie obviousness rejections.

A.1.2 Claims 1, 18, and 27 Are Non-Obvious in View of the References

In addition, claims 1, 18 and 27 are non-obvious in view of the references. Pereira is a security system that affects the basic levels of an individual computer's operating system. Win provides

centralized network security. If the methods of Pereira were incorporated into the methods of Win, then the user identity and privileges for each user at each computer would have to be set at boot-up for each individual computer. Thus, if users were to be changed at each computer, then each computer would have to be rebooted. If implemented over a network, one would have to reboot a local computer every time a new user is to gain access to a client computer. No one of ordinary skill would implement this system because it is slow, cumbersome, and wasteful of resources, time, and money. Thus, no one would be motivated to combine the references. Accordingly, the claims are non-obvious.

In addition, Pereira and Win are both relatively old references in the art of computer programs computers. The primary reference of Pereira issued in 1998 and Win issued in 2000. Pereira is about seven years old and Win is about five years old. In the art of managing resources on UNIX based systems, in view of the extremely rapid pace of development in the computer arts generally, seven years and five years represents a very long time. If it had been obvious to combine the references in the manner suggested by the examiner, then one of ordinary skill would have already done so, given the advantages that the claimed inventions have over the prior art. Therefore, claims 1, 18 and 27 are non-obvious over Pereira in view of Win.

A.1.3 Claims 1, 18, and 27 are Patentable over Pereira in View of Win

In summary, the examiner has failed to state prima facie obviousness rejections of claims 1, 18 and 27 because the proposed combination does not result in the claimed inventions, because the examiner has failed to state a proper motivation to combine the references, and because the examiner used impermissible hindsight to fashion the rejections. In addition, claims 1, 18 and 27 are non-obvious in view of the references because the proposed combination would be slow and

impracticable and because if combining the references had been obvious, then one of ordinary skill

would have already done so.

A.2 Claims 2 and 15

Regarding claims 2 and 15, the examiner asserts that:

> 10.   As per claims 2 and 15, Pereira and Win taught the invention
> substantially as claimed in claims 1 and 18 above. Win further taught
> wherein the contents of the configuration file are defined by a network
> administrator (col. 12, lines 45-50).

Office Action of October 22, 2004, page 4, paragraph 10.

Claims 2 and 15 depend from claims 1 and 13, respectively, and therefore should be allowable

for the same reasons given above. In addition, neither Pereira nor Win show a configuration file, as

discussed above, so neither Pereira nor Win can show an administrator defining the contents of the

configuration file.

The examiner asserts that Win does show the claim feature, citing the following text:

> Administration Application 114 is used by administrators to configure
> server components of the system, to set up user and resource records,
> assign roles to users and resources and manage changes to the system. The
> Administration Application provides these services by reading and writing
> information in Registry Server 108.

Win, col. 12, lines 45-50.

The examiner misapprehends Win. The cited text discusses configuring server components of a

system, setting up user and resource records, assigning roles to users and resources, and managing

changes to the system. However, the cited text does not discuss storing a configuration file on a

network server, as claimed. Pereira fails to cure the lack of disclosure in Win. Thus, the proposed

combination does not result in the claimed inventions. Accordingly, the examiner has failed to state

prima facie obviousness rejections of claims 2 and 15.

A.3 Claim 3

Regarding claim 3, the examiner asserts that:

> 11.   As per claim 3, Pereira and Win taught the invention substantially
> as claimed in claim 1 above. Win further taught wherein the configuration
> file is stored on a network server (col. 12, lines 2-6; col. 16, lines 43-54;
> col. 23, lines 20-23).

Office Action of October 22, 2004, page 4, paragraph 11.

Claim 3 depends from claim 1, and therefore is patentable over Pereira in view of Win as

discussed above. In addition, the examiner misapprehends Win. The cited text is as follows:

> Authentication Server Module 606 provides access to the Registry
> Repository 110, which stores User, Resource, and Role information.
> Access Control Library 610 also provides access to the Registry
> Repository.

Win, col. 12, lines 2-6.

> For example, consider a user who is defined in the Registry Repository as
> having a Record Type of User, a Record Name of Harvey, and a Role of
> Hotline Staff. A field in the Admin Role record specifies whether that user
> is assigned the "configuration privilege". This privilege allows an
> administrator to configure and maintain servers in the system. For
> example, the Registry Repository contains a record having a Record Type
> of Admin Role, a Record Name of Hotline Staff, a Configuration Privilege
> of No, and an Administration Privilege of HelpDesk Admin. Another field
> in the Admin Role record specifies the set of administrative functions that
> may be performed.

Win, col. 12, lines 43-54.

> In the preferred embodiment, Administration Application 114 can generate
> reports that list information stored in Registry Repository 110. For
> example, Administration Application 114 generates a Roles By Resource
> report that lists roles that are supported by specified resources.

Win, col. 23, lines 20-23.

As the cited text shows, Win does not teach wherein the configuration file is stored on a

network server because Win does not teach creating a configuration file in the first place.

Therefore, the examiner has failed to state a prima facie obviousness rejection of claim 3.

THIS PAGE LEFT BLANK